Journal of Theoretical and Applied Information Technology
20th December 2013. Vol. 58 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

BIOMETRIC BASED STRONG REMOTE USER AUTHENTICATION USING SMART CARD

[1]S.RAMESH, [2]DR.V.MURALI BHASKARAN
[1]Assistant Professor, Department of Computer Science and Engineering, Tamilnadu, India.
[2]Principal, Dhirajlal Gandhi College of Technology, Tamilnadu, India.
E-mail: [1]raameshs@gmail.com, [2]murali66@gmail.com

ABSTRACT

Remote user authentication is one of the major issues in the rapid growing internet era. In this paper we propose a biometric based remote user authentication scheme using smart cards. The existing methods failed to be safe in remote user authentication as the secret values in either end of the communication could be guessed by the intruder. In our scheme we introduce an addition security at the user side as an extra nonce by which the intruders will be unable to guess the users secret data. Hence our proposed scheme proves to provide a strong authentication and non-repudiation even in an insecure communication by sending and receiving messages with timestamps.
Keywords: *Biometrics, Smart card, Cryptography, Authentication, Security*

1. INTRODUCTION

The rapid development of Internet technologies legitimate users access the remote resources over the insecure communication channel by the use of user identity and password. User authentication is an essential security mechanism for remote system to assure one communicating party that validates the corresponding party. Three factors are considered before authentication take place.

1. What you know (password, PIN) 2.What you have (token, smart card, portable storage devices) 3.What you are (fingerprint, iris, face)[11]. There are numerous upcoming remote schemes are all are based on identity and password. In password authentication scheme the simple and easily breakable passwords are hacked by impersonation and dictionary attack. The long and random generated cryptographic keys are difficult to remember and stored in storage devices. Easily forgettable, lost and shared password, random generated cryptographic keys are unable to provide non repudiation and there is no way to know who the actual user is [1].

Biometric authentication is a procedure to identify the individuals based on biological and behavioral traits(finger print ,iris, face, palm print, retina, hand geometry, voice, signature and gait).Biometric authentication are reliable and secure than traditional password based authentication. Using biometric keys in the user authentication process have many advantages [3]

- Bio metric keys cannot be lost or forgotten
- Bio metric keys are very difficult to copy or share
- Bio metric keys are extremely hard to forge or distribute
- Bio metric keys cannot be guessed easily
- Bio metric keys are not easily to break

The smartcard based authentication is classified into hash based authentication and public key based authentication. This user scheme uses the user's personal biometrics along with his/her password with the help of the smart card. The user's biometrics is verified using BioHashing. This scheme is efficient due to usage of one-way hash function and exclusive-or (XOR) operations. XOR and concatenation operations require very few computations it is usually negligible considering its computational cost. Remote user authentication use nonce or long pseudorandom numbers and timestamps for better security and strong mutual authentication between user and server. Symmetric key crypto system is used in place of hash functions because the computational complexity of symmetric key

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

encryption and decryption is similar to hash function.

A secure and improved efficient biometrics based remote user authentication usually meet the following essential requirements

1.1 Security requirement:

To design remote user authentication that should be threatened by several security attacks at the same time to achieve the security goals such as confidentiality, integrity and availability. We discuss the following security attacks in order to analyze the remote user authentication scheme withstand the following attacks.

- Resist masquerade user attacks: An illegal user to impersonate as a legitimate user to correspond with a legitimate system.
- Resist masquerade server attacks: Attacker pretense as a legal system communicates with legal users. User assumes that attacker is a legal system.
- Resist parallel session attacks: Attacker and user access the system parallel manner.
- Resist stolen verifier or insider attacks: user's smart card has been lost or stolen by the attackers. Smart card contain contains significant information such as biometrics, hash algorithm and computed values.
- Resist password guessing attacks: Attackers assume the password using some dictionary words. During the communication between the server and client the password cannot leak out.
- Resist DOS attacks: Simultaneously access the system by multiple users but the system cannot respond to any incoming request.
- Resist replay attacks: Adversary intercepts the message between the user and the system and resend with modified message to the intend user.
- Resist man in middle attack: An attacker to impersonate as legitimate user while message interaction and create fake message as original message.
- Infringed account attack: An adversary intercept the login message and make use the significant information for re registration.
- Resembling account attack: An attacker creates attacks without limited number of times during registration process.

1.2 Functionality requirements:

- Users are allowed freely select and change the password in his/her side without the consultation of registration center or server this will reduce communication overheads and few security attacks in between both end of the communication parties. In a public insecure network.
- Certain remote schemes use timestamps to resist replay attack. It also lead to synchronization clock .problem
- Mutual authentication between client and server is established by generating session key on both ends.
- Do not maintain password and identity table in the system.
- Provide non repudiation by storing personal biometric information in a secured storage media.

1.3 Performance requirements:

Remote user authentication scheme use smart cards that do not assist high computational capacity. Hence scheme will not use exponential operation which incurs high computational cost. In message transmission on either end of communication take communication cost in terms of bits. Hence a good remote scheme will provide

- Low computational cost.
- Less communication cost.

In Li et al.'s scheme fails to provide proper authentication in login and authentication phase s because there is no verification on user's entered password after successful verification of his/her biometric template. We also show that due to the same password verification problem Li et al.'s scheme fails to update the new password correctly of a user in password change phase. The rest of the paper is organized as follows. Section 2 shows the related work of the remote user authentication scheme. In Section 3we review Li-et al.'s biometric based remote user authentication scheme using smart cards. Section 4 describes a cryptanalysis of Li-et al.'s scheme. The proposed remote user authentication scheme and the corresponding security, performance and functional analysis are discussed in sections 5,6 and 7 respectively. Finally we conclude this article in section 8.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. LITERATURE REVIEW

Remote user authentication is a security mechanism in a distributed network environment to identify the authenticated user by the remote server through identity and password. The first remote authentication scheme that store passwords in a verification table was proposed by Lamport(1981) for the public insecure network. In such scheme an adversary attempts to break the authentication mechanism by changing the password table at the server side. Later many schemes were modified to improve security, cost and efficiency.

Smart card based non interactive password authentication scheme without using verification table was proposed by Hwang Chen and Laih (1990). Other enhanced password authentication schemes were proposed by Chang and Wu (1991), Haller (1994) and Wang, Cheng (1996) modified the Lamport scheme that cannot resist the interpolation attacks. Many of the proposed schemes improved the computational cost and security (Yeh and Li 1997) but they were unable to withstand the impersonation attack. A scheme without using password table and introducing a computation on both of the communication parties that make the mutual authentication was proposed by Jan and Chen (1998).Hwang and Li (2000) introduced smart card to identify the individual in the client side in remote user authentication scheme. Collision resist hash functions were used for secured communication in an insecure network by Peyravian and Zunic (2000).Server maintains a public key for security improvement in authentication scheme proposed by Hwang and Yeh (2002). Smart card store the fingerprint, hash function and few computations for personal verification at user side was incorporated for further level of security development in remote user authentication scheme by Lee (2002).

Yoon (2005) proposed efficient and secure fingerprint based remote user authentication scheme using smart card that resist the vulnerability to forgery attack that was not easily repairable. In 2006 MK Khan and Zang redefined the authentication scheme that resist server spoofing attack and supported for mutual authentication. Secure remote user authentication scheme proposed by Kim (2009) eliminate the insidious attacks such as masquerade user and server attacks. Parallel session attack and password guessing attack in the previous schemes were eliminated by Hsiang and Shih (2009). In 2010, Li Hwang proposed an efficient biometric based remote user authentication scheme using smart cards. Efficiency is achieved by using one way hash functions, bio metrics, smart card and nonce instead of time stamp. Li et al (2010) pointed out that Li Hwang et al did not provide proper authentication and could not resist man in middle attacks (2011). Li et al scheme was insecure in terms of password communication and changing it locally without consulting registration center. A.K...Das et. al (2011) showed that flaws in login and authentication phases of Li-Hwang's remote authentication scheme can be avoided with biometrics verification using hash function. Eon(2011) described an enhanced biometrics remote user scheme that use symmetric encryption with hash function to reduce the computational cost and remove the man in the middle attack without the use of database. The remote user authentication was improved by exploiting hash functions which removed the infringed account attack and resembling account was proposed by Wen.(2012).Our proposed scheme provide the facility of encrypting message while the messages transmit over insecure channel that avoid the man in middle attack and eliminate replay attack. Introduce extra nonce at the user side also facilitate our scheme withstand against any guessing attack.

3. REVIEW OF LI-ET AL.'s REMOTE USER AUTHENTICATION SCHEME

The notations are used throughout this paper can be summarized in Table 1.We review Li et al.'s biometrics based remote user authentication scheme using smart cards.

Table 1: Notations used in the proposed scheme

Symbol	Description
C_i	Client or User
S_i	Server
R_i	Trusted Registration Center
ID_i	User i's Identity
SID_i	Server i's Identity
PW_i	C_i's Password
B_i	C_i's Biometric template
h(.)	One way hash function
$E_k()$	Symmetric Key Encryption
$D_k()$	Symmetric Key Decryption
X_s	Server S_i's secret key
X_c	User or ClientC_i's secret key
R_c	User or Client C_i'srandom number
R_s	Server S_i's random number
||	Concatenation operator
⊕	XOR operator

Journal of Theoretical and Applied Information Technology
20th December 2013. Vol. 58 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Li et al.'s scheme consists of four phases that are registration phase, login phase, authentication phase and password change phase

3.1 Registration phase

The remote user C_i login to the system the user initially registered with server and performs the following activities.

Step 1:C_i select a random number N and computes the masked password $RPW_i = h(N \| PW_i)$ then input his/her personal biometrics on the specific device.

Offer identity ID_i and masked password RPW_i to registration centre $R_i$via a secure channel.

Step 2: The Registration centreR_i compute r_i and $e_i$as follows

$r_i = h(RPW_i \| f_i)$

$e_i = h(ID_i \| X_s) \oplus r_i$ where $f_i = h(B_i)$and ,X_s is Server secret key shared between R_i and S_i

Step 3: R_i store ID_i,h(.),f_i,$e_i$and y on the user smart card and sends it to the user C_i via a secure channel.

Step 4: Client C_i put N into his/her smart card.

3.2 Login phase

User login to remote server user perform the following activities.

Step 1 .User C_i inserts his/her smart card into the card reader and input his/her personal biometrics Bi on a specific device for verification. The f_i in the smart card has been compared with B_i. If the condition does not satisfy user C_i does not pass the biometric verification and the user authentication scheme is terminated. Condition satisfies means user passes the biometric verification.

Step 2: Then user C_i inputs the ID_i and the password PW_i.The smart card receives the password PW_i, it perform the following computations

$RPW_i = h(N \| f_i)$

$r_i = h(RPW_i \| f_i)$

$M_1 = e_i \oplus r_. = h(ID_i \| X_s)$

$M_2 = M_1 \oplus R_c$ where R_c is C_i generate a random number.

$M_3 = h(y \| R_c)$

$M_4 = RPW_i \oplus M_3$

$M_5 = h(M_2 \| M_3 \| M_4)$

Step 3: C_i sends the message $<ID_i, M_2, M_4, M_5>$to the remote server S_i.

3.3 Authentication phase

Server receive the request login message from the user, it verify the user is legal or not and perform the following actions.

Step 1: Server S_i validate the format of ID_i or not.

Step 2: If ID_i is valid one S_i compute the following message for mutual communication between the server and user.

$M_6 = h(ID_i \| X_s)$

$M_7 = M_2 \oplus M_6 = R_c$

$M_8 = h(y \| M_7)$

Verify $M_5 = h(M_2 \| M_8 \| M_4)$.If both are equal S_i stores (ID_i, M_7) in the data base. Server receive C_i's next request login message, server S_i compute M_7'.Server compare M_7' against M_7 stored in the database. If both values are same then the server assumes there is a chance of replay attack. Hence it rejects the request the login message. If not S_i stores M_7' in the database to restore M_7. . By using this database technique to resist the replay and man in middle attacks.

Step 3: If step 2 does not hold, server rejects login request and conclude the current session. Otherwise Si accepts C_i is an authenticated user. Si computes

$M_9 = M_4 \oplus M_8$,

$M_{10} = h(M_9 \| SID \| y) \oplus M_8 \oplus R_s$

$M_{11} = h(M_6 \| M_9 \| y \| R_s)$ Where R_s is server generates a random number.

Step 4: S_i sends the message (M_{10}, M_{11}) to the user C_i.

Step 5: User C_i receive the message from Server $S_iC_i$computes$M_{12} = h(RPW_i \| SID_i \| y) \oplus M_3 \oplus M_{10}$and verifies$M_{11} = h(M_1 \| RPW_i \| y \| M_{12})$.

Step 6: If it holds User C_i accepts S_i is an authenticated server .Otherwise Ci ends the scheme. After the mutual authentication phase, User C_i and Server S_i compute $h(RPW_i \| SID_i \| M_3 \| M_{12})$ and $h(M_9 \| M_8 \| R_s \| SID_i)$,these are considered as session key respectively. In this computation if$<ID_i, M_2, M_4, M_5>$ and $<M_{10}, M_{11}>$ are valid messages $M_9 = RPW_i$,$M_8 = M_3$,$M_{12} = R_s$ and $h(RPW_i \| SID_i \| M_3 \| M_{12}) = SK = h(M_9 \| M_8 \| R_s \| SID_i)$

3.4 Password change phase

If user C_i wants to change his/her old password PW_i to a new password PW^{new} freely without the consulting Registration center R_i. Then user C_i does the following steps.

Step 1: User C_i insert his/her smart card into the card reader.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step 2: Next input his/her biometric template Bi on the specific device to verify user Ci biometrics.
.
Step3: If h (B_i) matches with f_i then passes the verification process happens.
Step 4: User C_i enters his/her old password PW_i and new password PW_i^{new}. Next smartcard will perform the following operations

$RPW' = h(N||PWi)$
$r_i' = h(PW_i||f_i)$
$e_i' = e_i \oplus r_i'$
$RPW_i^{new} = h(N|| PW_i^{new})$
$r_i'' = h(PW_i^{new}|| f_i)$
$e_i^{new} = e_i' \oplus r_i''$

Finally e_i^{new} is replaced with newly calculated value e_i on the smartcard.

4 CRYPTANALYSIS OF LI-ET. AL'S REMOTE USER SCHEME

In this remote scheme attackers create attacks by intercepting and interpolating the messages while transmitted via insecure channel in login and authentication phases.

Fail to provide strong authentication:

In login phase of Li et al.'s scheme the user C_i enter his/her biometrics on specific device to verify whether his/her biometrics passes or not. If verification is correct then C_i enters his/her identity ID_i and password PW_i. There is no password checking process in login phase. [3]. If the user enters wrong password the login and authentication phase still continue. At the end of authentication phase Si rejects the login request. In this juncture extra communication and computational cost were increased in login and authentication phases. These events may not know by the user Ci.

By crypt analysis C_i enters wrong password (PW'). PW≠PW' [5]

$RPW_i = h(N||PW_i') \neq h(N||PW_i)$
$r_i' = h(RPW_i'||f_i) = h(h(N||PW_i') || f_i)$
$\neq h(h(N||PW_i') || f_i)$
$M_1 = e_i \oplus r_i' \neq h(ID_i||X_s)$
$M_2 = M_1 \oplus R_c \neq h(ID_i||X_s) \oplus R_c$
$M_3 = h(y || R_c)$
$M_4 = RPW_i \oplus M_3 \neq h(N||PW_i) \oplus h(y || R_c)$
$M_5 = h(M_2 || M_3 || M_4)$
$\neq h(ID_i||X_s) \oplus R_c || h(y||R_c) || h(N||PW_i)$
$\oplus h(y || R_c)))$

After sending message <IDi, M_2, M_4, M_5> Si compute

$M_6 = h(ID_i||X_s)$
$M_7 = M_2 \oplus M_6 \neq R_c$
$M_8 = h(y||M_7) \neq h(y || R_c)$

S_i compares M_5 with $h(M_2 || M_3 || M_4)$
Si does not store <ID_i, M_7> in the database and reject the login request and terminate the session. C_i does not authenticate as a valid by user S_i.

Man in Middle attack or Impersonation attack

Attacker captures the message in login and authentication phase in order to impersonate as one of the communicating party. Both the end parties of the communication think that the other end is a authenticated one. The messages are transmitted over an insecure channel. Therefore there is a chance for man in middle attack or impersonation attack. Attacker proceeds like as User and C_i sends the message <ID_i, M_2> to S_i. An adversary A eavesdrops the message <ID_i, M_2'> and send this message as <ID_i, M_{A2}> to S_i. S_i received the message and selects a random number R_{AS}

Password Guessing attack:

An adversary A try to guess or steal the password of the user in the login phase. There is no password check before the computation of r_i and e_i.. Even the user enter wrong password in the login and the authentication phase still continues. This includes extra communication and computational overheads [5]. In the cryptanalysis user enter the wrong password PW_i' in the login phase and calculation the messages M_1, M_2, M_3, M_4 and M_5. There is no password checking procedure before the messages were calculated. The incorrect messages sent to the server and compute the messages M_6, M_7, M_8 using M_2 in the authentication phase.

Replay attack:

In the authentication phase the eavesdropper intercept the login message <ID_i,M_2,M_4,M_5> from the previous session which one is not most recent session of the user. The eavesdropper login to the server S_i with the eavesdropped message ,S_i check the validity of ID_i and compute M_6,M_7 and M_8.The S_i verifies the equation M_5 and compares recent M_7 to M_7' in the database. If M_7 differs from M_7' S_i considers the login request as a legal one and store current sessions M_7 to the database. At last Si authenticates the attacker and computes M_{10}, M_{11} and sends to attacker. So that attacker can act as Ci through replay attack.

Stolen verifier attack:

All existing confidential information stored in the smart card leads to this attack. An adversary leak the significant information such as ID_i,h(.),f_i,e_i and y to illegal user. The secret key y and hash functions of the remote server is known

Journal of Theoretical and Applied Information Technology
20th December 2013. Vol. 58 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

by an attacker easily manipulate the other computation such as fi,ei and $r_{i..}$

5. PROPOSED SCHEME

Our proposed remote user authentication scheme contains 6 phases which is described in the following section

5.1 Setup phase

Setup phase consist of 3 steps.
Step 1: Server setup: This process is performed by Server Si the Random number R_s chosen by S_i.
Step 2: Client Setup: Client initializes the Random Number (X_c) for masking password and the number R_c chosen by C_i.
Step 3: System Setup: The Registration center R setup the overall environment to publish hash function h (.), symmetric encryption, decryption function $E_k()/D_k()$ and message authentication code(MAC).Distribute X_s to Server S_i through secure channel.

5.2 Registration phase

An interaction between Registration Centre R_i and Client C_i done before the login process starts. The remote user performs the following steps.
Step 1: C_i selects the random number X_c and it is depicted in Figure 1.
Step 2: C_i inputs his/her personal biometrics B_i on the specific device and provides the password PW_i, identity of the user $ID_{i.}$.
Step 3: User C_i provides ID_i,PW_i to registration center R_i via a secure channel (in person).
Step 4: Registration center R_i compute f_i,r_i and e_i
$f_i = h(B_i)$
$r_i = h(PW_i \oplus X_c || f_i)$
$e_i = h(ID_i || X_s) \oplus r_i$
Step5:Registration enter R_i stores f_i,r_i,e_i,v_i,$h(.)$,$E_k()/D_k()$ on C_i's smart card and sends it to $C_i$via secure channel.
Step 6: User C_i enters X_c into his/her smart card.

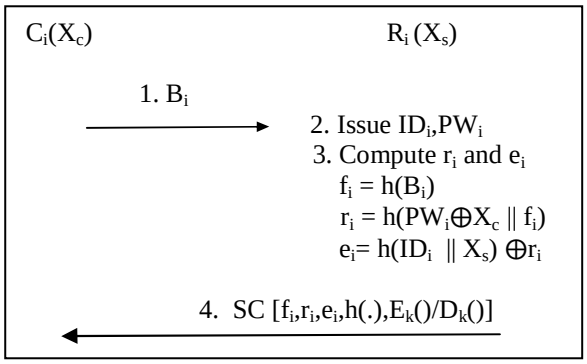

Figure 1: Registration Phase

5.3 Reregistration phase

Step 1: If user C_i loses or misses his/her smart card and need to re-register to server S_i.
Step 2: User chooses a new random number X_c'.
Step 3: User sends ID_i, PW_i to the registration center R_i.
Step 4: Registration center R_i compute f_i,r_i and e_i

$f_i = h(B_i)$
$r_i = h(PW_i \oplus X_c || f_i)$
$e_i = h(ID_i \oplus X_s) \oplus r_i$

Step5: Registration center R_i stores f_i,r_i,e_i,$h(.)$,$E_k()/D_k()$ on C_i's smart card and sends it to C_i via secure channel.
Step 6: User C_i enters X_c into his/her smart card.

5.4 Login phase

After registration gets over the user C_i wants to logon to the remote server S_i, he/she perform the following steps and represented diagrammatically in Figure 2.
Step 1: C_i inserts his/her smart card into the card reader.
Step 2: Next input his/her personal biometrics B_i on the specific device.
Step 3: Verify his/her biometrics by h (B_i) = f_i.
Step4: If the above verification does not hold C_i terminate the current remote user authentication.
Step5: Or else the verification was success C_i passes biometric verification and then C_i input his/her login id ID_i, and password PW_i.

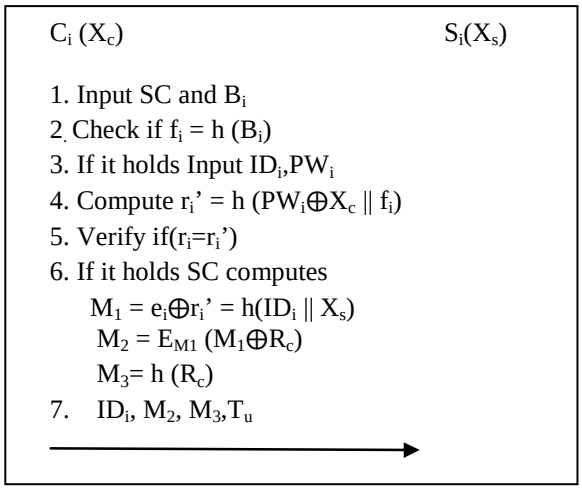

Figure 2: Login Phase

Step 6: The smart card computes the following
$r'_i = h (PW_i \oplus X_c || f_i)$
Step7: Compare r_i and r_i' . If $r_i' \neq r_i$ then password verification fails and terminate current user session.

Journal of Theoretical and Applied Information Technology
20th December 2013. Vol. 58 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step8: If $r_i = r_i'$ the smart card compute the following operations

$M_1=e_i \oplus r_i' = h (ID_i \| X_s)$

$M_2= E_{M1} (M_1 \oplus R_c)$ Where R_c is user generated random number.

$M_3=h (R_c)$, Where M_3 is the authentication code for M_2.

Step9: Lastly C_i sends $<ID_i, M_2, M_3, T_u>$ message. Where T_u is the user's current time stamp.M_3 is used to achieve message integrity while the communication takes place. Any attacker does not eavesdropping the message.

5.5 Authentication/Verification phase

This is an agreement between the user and server after the successful completion of login process before the message communication starts. The server receive the login request message$<ID_i, M_2, M_3, T_u>$ from the user to identify C_i is a legal user or not.

Step 1: Server check the format of ID_iorT_u is invalid or T_s-T_u<=0.If it holds S rejects user login request.

Step 2: If it does not holds S_i computes

$M_4 = h (ID_i \| X_s)$ (= M_1)

$M_2' = D_{M4} (M_2)$ (= $M_1' \oplus R_c$)

$M_5 = M_2' \oplus M_4 = R_c$

Step 3: Server S_i verify whether if M_3 equals $h(M_5)$

Step4: If it does not holds then Server S_i reject user request. If it holds Server $S_i$computes

$M_6 = E_{M4} (M_4 \oplus R_s)$

$M_7= h (R_s)$

Step 5: S_i sends the message $<M_6, M_7, T_s>$ to user C_i. Where $M_7$is the authentication code for M_6

Step 6: If either Ts is invalid or $T_s=T_u$, the session comes to end by user C_i.

Step 7: Otherwise user decrypts M_6. $M_6' = D_{M1} (M_6)$.

Step 8: User compute $M_8=M_6' \oplus M_1 = R_s$

The diagrammatic explanation is given as below

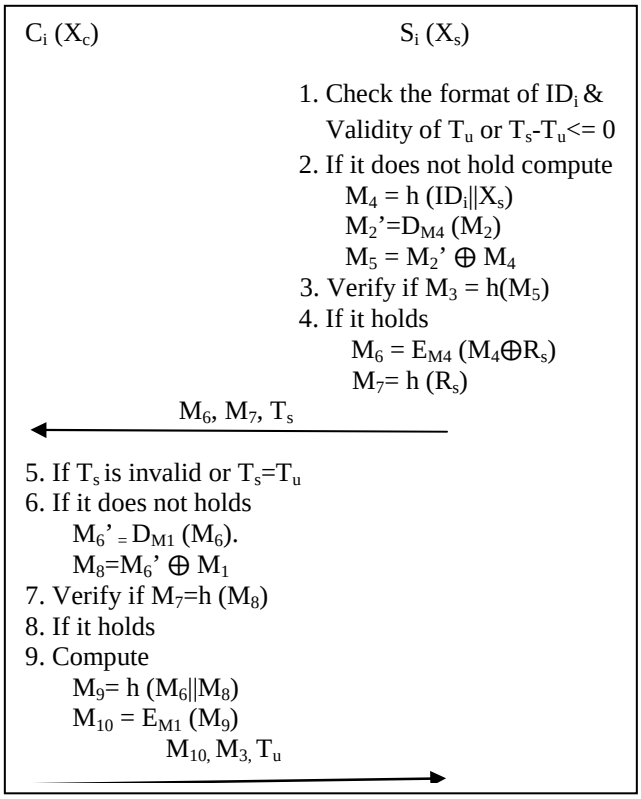

Figure 3: Authentication Phase

Step 9: User verifies whether $M_7=h(M_8)$ .If it does not hold terminate the user session.

Step 10: If it holds user C_i compute

$M_9=h (M_6 \| M_8)$

$M_{10} = E_{M1} (M_9)$

Step 11: User C_i sends messageM_{10}, M_3,T_u to S_i. Here $M_3$is the authentication code for $M_{10.}$

Step 12: Or else ends the user's current session.

5.6 Secret key Generation phase

Step 1: After receiving users message, S_i verifies if T_s is invalid or T_s-T_u<= 0 terminate the user session.

Step 2: Otherwise S_i decrypts M_{10}

$M_{10}' = D_{M4} (M_{10})$

Step 3: Another verification by whether M_{10}' = $h(M_6 \| R_s)$ and $M_3 = h(M_5)$

Step 4: if it holds accept C_i login request else reject user login request.

Step 5: After the mutual authentication the user compute the session key as $h(M_1 \oplus R_c \oplus M_8 \oplus SID)$ and server compute the session key as $h(M_4 \oplus M_5 \oplus R_s \oplus SID)$.

Step 6: By the use of the session key the user and server further continue with their communication.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

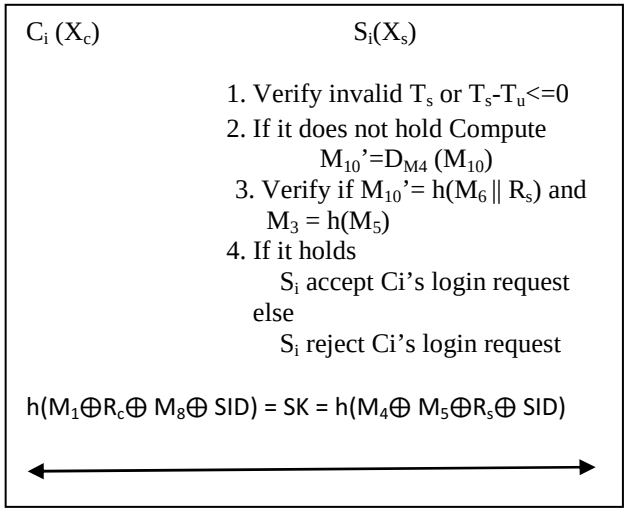

Figure 4: Session key generation Phase

5.7 Password change or updating phase

When the user wants to change his/her password with new password freely without contacting the remote center R_i he/she have to enter into this phase. After the biometric verification there is a chance to enter wrong old password by mistake. Then the value of e_i was updated that have incorrect value. If the user wants to login the system with new password, the server rejects the users request and reports that that it is incorrect password and ask again to re login. But the smart card verify the old password entered by the user before update e_i,r_i in it. This phase perform the following steps.

Step 1: Insert his/her smart card and input his/her biometric template.

Step 2: Compare h (B_i) with f_i.

Step 3: Both values are same C_i passes the biometric verification.

Step 4: Send a User request to Server to offer to change password by make use of session key.

Step 5:.If it accepts C_i enter his/her old password PW_i and new password PW_i^{new}.

Step 6: Smart card compute $r_i'=h(PW_i \oplus X_c \| f_i)$

Step 7: If $r_i' \neq r_i$ then $C_i$enter his/her wrong old password.

Step 8: If $r_i=r_i'$

$r_i'' = (PW_i^{new} \oplus X_c \| f_i)$

$e_i' = e_i \oplus r_i'$

$e_i'' = e_i' \oplus r_i''$

Step 9: Replace e_i with e_i'' and r_i with r_i'' on the smart card.

6 SECURITY ANALYSIS

In this section we analyze the security of the proposed scheme and discuss the security features involved in it.

6.1 Secret Key Security

In our system the remote server maintains two pieces of secret information X_s and R_s. X_s is only manipulated by S_i. Client also maintains its own secret key R_c and X_c which is not publicly available. An attacker may try to derive X_s from the login message $<ID_i, M_2, M_3, T_u>$ in the login phase and $<M_6, M_7, T_s>$ in authentication phase. Hence it is infeasible to compute the hash function and break the symmetric encryption.

6.2 Impersonate Attack/ Masquerade On Client And Server Side

In our proposed system an illegal user try to intercept and fabricate the login request message $<ID_i, M_2, M_3, T_u>$ of C_i in the login phase that cheat the remote server as a valid user . It is impossible to compute the message M_2 and M_3 by the illegal user in order to convince S_i unless he/she knows the secret information R_c. The server also reply with $<M_6, M_7, T_s>$ message to the user. Again there is no possibility of any invalid user impersonate as like server because all are encrypted messages with secret values maintain on both end.

6.3 Resist Replay Attack

To perform a replay attack an adversary E eavesdropped message $M_2$from C_i which is not the last session .E create a fake message M_2' and send to S_i. S_i respond to E with $M_6' = E_{M4}(M_4 \oplus R_s)$ .But E cannot decrypt M_6' without knowing the value of R_s..Here we do not use database that store the ID and R_c values that can be easily attacked by the adversaries. So there is a chance for trace the client secret number R_c.

6.4 Resist Man In Middle Attack

The adversary cannot dissect the login and authentication messages because all the messages are encrypted with unknown hash code as key value. These messages are sent along with the message authentication code. No messages are altered that can be easily detect at the other end.

6.5 Strong Mutual Authentication

Our scheme can provide strong mutual authentication that can enable by client C_i send

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the login message <ID_i, M_2, M_3> to server S_i. The server S_i checks the validity of ID_i and timestamps that ensure the authenticity of the client. Then compute M_4, M_5 and again authenticate C_i by verifying M_3 with $h(M_5)$. If it holds user C_i is a valid user. Otherwise user C_i does not pass the authentication. Any fake message cannot pass in the authentication phase. Server Si sends messages M_6 and M_7 to the user C_i. Next Ci compute M_8 and compare $h(M_8)$ with M_7 to provide a level of authentication. User C_i calculates M_{10} and encrypted it and sends it to the server S_i .Final level of authentication is done by compare $h(M_6 \| R_s)$.Therefore any fabricated message cannot pass the authentication.

6.6 Stolen verifier attack

In Li et al. and Das et al. scheme store identity and R_c into user database. Hence there is a chance for replay attack. The proposed scheme is not used any user database that store the users identity, passwords and users nonce value. Hence there is no threat against stealing any significant information from the system.. In our scheme we do not maintain any table but we use timestamps to withstanding the replay attack.

Table 2 shows the security comparison of our scheme with other related schemes.

Table 2: Security Comparisons

Security Factors	Li-Hwang[10]	Li et. Al[11]	Das et.al[11]	Proposed scheme
Biometric authentication	No	Yes	Yes	Yes
Password checking before computation	No	No	Yes	Yes
Replay resistance without use of Database	No	No	No	Yes
Session key agreement	No	Yes	No	Yes
Security in insecure channel	No	No	No	Yes

7 PERFORMANCE AND FUNCTIONALITY ANALYSIS

In this section we evaluate the performance and functionality of the proposed scheme and compare with those of Li-Hwang et al.'s scheme and Li et al.'s scheme. We analyze the results of computation and communication cost in terms of hash function but without exclusive OR operation and concatenation operation. Because XOR and concatenation operations require very few computations it is usually negligible considering its computational cost. In our scheme we use a symmetric key cryptosystem for communicating message over a insecure communication channel. The computational complexity of a symmetric key encryption or decryption operation is similar to the hash function operation. The AES-256 scheme is more efficient than SHA-256 scheme in resource constrained devices. The message communication between user and server of our scheme is same as that of Li-Hwang scheme and Das et al.'s scheme which have 3 insecure communications. But in Li et al.'s scheme has 2 insecure communications. If communication cost is low then that leads to vulnerable in parallel attack and replay attack. Table 3 shows the performance comparison of our scheme with other related schemes.

Table 3: Performance Comparisons

Phases	Li-Hwang et.al [10]	Li et. al [11]	Das et.al [11]	Proposed scheme
RP	3H	4H	3H	3H
LP	2H	4H	2H	2H
AP	5H	7H	8H	4H⊕4E
Total	10H	15H	13H	9H⊕4E

H – one way hash function
E - Symmetric encryption for insecure channel
RP – Registration Phase
LP-Login Phase
AP – Authentication Phase

The proposed scheme utilizes the length of the user's identity and password is 128 bits. The length of every random number produced by the random number generator is 256 bits and the length of the timestamp is about 64 bits. The

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

memory needed in the smart card for each parameter is 128 bits. Our scheme provides the user anonymity by an attacker intercepted the login message $<ID_i, M_2, M_3>$,then the attacker may try to retrieve any static parameter from these messages, but M_2, M_3 are all session variant and indeed random strings due to the randomness of R_c.. This scheme has session key agreement phase for generating session keys at the both ends.. In that client generate a session key and server produce a session key. If both the session keys are same then further communication continues.

In our scheme the session key SK = $h(M_1 \oplus R_c \oplus M_8 \oplus SID) = h(M_4 \oplus M_5 \oplus R_s \oplus SID)$ is associated with R_s, R_c and hash values. In this scheme the adversary cannot trace the user activity as all the messages are transmitted in encrypted form. It prevents any adversary acquiring sensitive information such as server identity in the session agreement phase. The proposed method also has the facility to change the password freely by using new password to replace the new values of r_i and e_i. in the smart card. In our scheme in all phases client C_i and server S_i communicate each other by creating a timestamp and sender's identity's hash value for achieving non repudiation. Moreover we summarized the functionality of the proposed scheme and compare with other schemes in Table 4, which clearly shows that our scheme is more secure than others.

Table 4: Functionality Comparisons

Functional Factors	Li-Hwang[10]	Li et. al.[11]	Das et.al[11]	Proposed scheme
Password Change freely	Yes	Yes	Yes	Yes
Strong Mutual authenticatio n	No	Yes	No	Yes
Provide non repudiation	Yes	No	No	Yes
User anonymity	No	Yes	Yes	Yes
Provide session key agreement	No	Yes	No	Yes

8. CONCLUSION

In this paper a new biometric based user authentication scheme using smart card has been proposed. The proposed scheme improves Li et al.'s scheme in order to provide strong authentication and non-repudiation and defend against the replay attacks, man in middle attacks, and stolen verification attacks. The proposed scheme updates the password freely without the knowledge of registration center. Our scheme has double security protection mechanism where message are transmitted over an insecure channel. When compared with other schemes our scheme enhances the security in terms of security goals.

REFRENCES:

[1] Lamport.L., , "Password authentication with in secure communication", *Communications of the ACM*, Vol 24, No 11,1981, pp. 770-772

[2] Li C-T, Hwang M S, "An online biometrics based secret sharing scheme for multiparty cryptosystem using smartcards", *Journal of Innovative Computing Information and Control* ", Vol. 6, No. 5, 2010a, pp. 2181-2188.

[3] Chun-Ta Li, Min-Shiang Hwang, "An efficient biometrics based remote user authentication scheme using smart cards", *Journal of Network and Computer Applications"*, Vol. 33, No. 1, 2010b, pp. 1-5.

[4] Li X, Niu J-W, Ma J., Wang W-D, Liu C.L "Cryptanalysis and improvement of a biometrics- based remote user authentication scheme using smart cards", *Journal of Network and Computer Applications*,Vol. 34, No 1, 2011,pp.73-79.

[5] A.K.Das "Analysis and improvement on an efficient biometric based remote user authentication scheme using smart cards",*IET Information Security"*, Vol 5, No 3, 2011,pp. 145-151.

[6] Sandeep K Sood, Anil K Sarie and KuldipSingh, "A Secure dynamic identity based authentication protocol for multiserver environment", *Journal of Network and Computer Applications"*, Vol. 34, No. 2, 2011, pp. 609-618.

[7] DebioHe,ShuhuaWu"Security Flaws in a smart card based authentication scheme for multi-server environment", *Wireless Personal*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Communications, Springer, Vol 70,2013 Issue 1 pp 323-320.

[8] Jing Chao "An improved remote password authentication scheme with smart card", *Journal of Electronics(China)*, Springer, Vol 29,Issue 6,2012 pp 550-555.

[9] Younghwa An "Improved biometrics based remote user authentication scheme with session key agreement", *Communications in Computer and Information Science* ,Vol 351,2012 pp. 307-315.

[10] Chun-I Fan and Yi-HuiLin "Provably secure remote truly three factor authentication scheme with privacy protection on biometrics", *IEEE Transactions on information and forensics and security*, Vol4 ,No 4 2009 pp. 933-945.

[11] Wang Ding MA Chun guang "Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards", *Journal of China Universities of Posts and Telecommunications*, Vol 19, No. 5 2012 pp. 104-114.

[12] A.K.Awasthi and S.Lal" An enhanced remote user authentication scheme using smart cards", *IEEE Transaction on Consumer Electronics* ,Vol 50 2,May 2004 pp. 307-315.

[13]Eun-Jun Yoon ,Kee-Young Yoo "Secure Fingerprint based remote user authentication scheme using smart cards",*Internet and Network Economics LNCS Springer*,vol 3828,2005, pp. 405-413.

[14] M K Khan ,JiashuZiang"An efficient and practical fingerprint based remote user authentication scheme with smart cards", *Information Security Practice and Experience LNCS Springer*, Vol 3903,2006 pp. 260-268.

[15] Ali A.Yassin ,Ha Jin, Ayad Ibrahim, DeqingZou"Encrypted remote user authentication scheme using smartcards", *Web Information Systems and Mining LNCS Springer*, Vol 7529,2013 pp. 314-323.

[16] Youngwa An "Security analysis and enhancement of an effective biometric based remote user authentication scheme using smartcards", *Journal of Biomedicine and Biotechnology* , Vol 2012 ,2012 pp. 314-323.

[17] Kuo-HuiYeh, ChunhuaSu,N.W.Lo,Yingjiu Li, Yi-Xiang Hung "Two robust remote user authentication scheme using smartcards", *Journal of Systems and Software* , Vol 83(12),2010, pp. 2556-2565.

[18] Cheng-Chi Lee, Cheng-Wei Hsu" A Secure biometric based remote user authentication scheme with key agreement using chaotic maps", *Journal of Nonlinear Dynamics*, Vol71(1) ,2013 pp. 201-211.

[19] Sang-KyunKim, Min Gyo Chung "Moresecure remote user authentication scheme", *Journal of Computer Communications*, Vol32 ,2009 pp 1018-1021.

[20] Wen-Bin Hseih, Jenq-ShiouLeu ,"Exploiting hash functions to intensify the remote user authentication scheme", *Journal of Computers and Security* , Vol 31 ,2012 pp. 791-798.